

Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey

Year: 2022 | Citations: 177 | Authors: Mansoor Ali, Faisal Naeem, M. Tariq, Georges Kaddoum

Abstract

Recent advances in electronic devices and communication infrastructure have revolutionized the traditional healthcare system into a smart healthcare system by using internet of medical things (IoMT) devices. However, due to the centralized training approach of artificial intelligence (AI), mobile and wearable IoMT devices raise privacy issues concerning the information communicated between hospitals and end-users. The information conveyed by the IoMT devices is highly confidential and can be exposed to adversaries. In this regard, federated learning (FL), a distributive AI paradigm, has opened up new opportunities for privacy preservation in IoMT without accessing the confidential data of the participants. Further, FL provides privacy to end-users as only gradients are shared during training. For these specific properties of FL, in this paper, we present privacy-related issues in IoMT. Afterwards, we present the role of FL in IoMT networks for privacy preservation and introduce some advanced FL architectures by incorporating deep reinforcement learning (DRL), digital twin, and generative adversarial networks (GANs) for detecting privacy threats. Moreover, we present some practical opportunities for FL in IoMT. In the end, we conclude this survey by discussing open research issues and challenges while using FL in future smart healthcare systems.